WHAT IS CLAIMED IS:

1. A security method for controlling use of an executable application, said method comprising the steps of:

procuring a software executable policy enforcement agent which, when invoked, imposes one or more conditions on successful execution, and which, when successfully executed, invokes execution of said executable application;

encapsulating said executable application with said policy enforcement agent without changing said executable application, to thereby produce a combined program;

substituting said combined program for said executable application, so that said policy enforcement agent executes instead of said executable application program when said executable application is invoked; and

one of (a) satisfying said conditions of said control module, whereby said executable application executes, and (b) not satisfying said conditions, whereby said executable application does not execute.

2. A method according to claim 1, wherein said software executable policy enforcement agent includes a header component, and said substituting step includes the step of amending said header component of said policy enforcement agent portion of said combined program to match the characteristics of said combined program.

3. A method according to claim 1, wherein said executable application includes a VPN-tunnel-generating application, and said step of satisfying said conditions includes the step of running an antivirus program.

4. A method according to claim 1, wherein said executable application includes a VPN-tunnel-generating application, and said step of satisfying said conditions includes the step of running a antivirus program having an acceptable update status.

5. A method according to claim 1, wherein said step of satisfying said conditions includes the step of running a personal firewall program.

6. A method according to claim 1, wherein said executable application accepts verification information in a format other than a digital certificate, and said step of satisfying said conditions includes the step of accepting a digital certificate.

7. A method according to claim 6, wherein said step of accepting a digital certificate includes the step of accepting an X.509 based digital certificate.

8. A method according to claim 6, further comprising the step of translating at

least some information from said digital certificate into a form recognizable by said executable application.

9. A method for policy enforcement in relation to an executable application, said method comprising the steps of:

procuring a software control element which is identifiable to a host operating system as an executable program and which includes an execution component for executing said executable application, and which also contains a set of conditions which must be met in order to invoke said executable application;

combining said software control element with said executable application, to form a combined program;

substituting said combined program for said executable application;

commanding execution of said combined program, to thereby execute said software control element, whereupon said execution component is invoked if said conditions are met, and said executable application executes.

10. A method according to claim 9, wherein software control element includes a header identifying the locations of executable and data portions of said control element, and said step of combining said software control element with said executable application includes the steps of:

appending said executable application

to said software control element in a location identified by said software control element as a data location; and

updating said header of said software control module to correspond with the characteristics of said combined program.